



THE UNIVERSITY  
of NORTH CAROLINA  
at CHAPEL HILL

OFFICE OF THE CONTROLLER    T 919-962-1370  
104 AIRPORT DR., SUITE 3200    F 919-962-4140  
CAMPUS BOX 1270  
CHAPEL HILL, NC 27599-1270

## MEMORANDUM

To: University Business Managers

From: Dennis Press  
University Controller

Date: August 8, 2006

Re: Compliance with Credit Card Merchant Services Policy

My purpose in writing is to provide information on changes in the State's credit card processing services and guidance on ensuring compliance with PCI (Payment Card Industry) data security standards. The State Controller notified us by a memorandum dated August 1, 2006 that the credit card processing services contract for the State has been awarded to the current vendor, SunTrust Merchant Services, LLC. Contract enhancements include reduced fees for merchants (i.e. campus departments that accept payments by credit card), Point of Sale (POS) terminal supplies at no cost, and other benefits. Another stipulation of the agreement requires all merchants, including campus departments, to be compliant with PCI data security standards no later than October 31, 2006.

The University's policy on credit card merchant services was distributed last month as explained in the attached copy of the memorandum dated July 12, 2006. The memorandum provides a link to the policy. Credit card merchant information for University departments can also be accessed at <http://www.unc.edu/finance/controller/fc/MerchCCard.htm>. Section D.4 of the policy notes that compliance with security standards for merchants is required. The policy states:

*All credit card merchants shall be compliant with the Payment Card Industry (PCI) Data Security Standards. Based upon the merchant level determination, the PCI has defined the compliance validation requirements. However, the Office of the State Controller is requiring merchants at all levels to complete the annual self-assessment questionnaire and to perform the required network scans for all externally-facing IP addresses. University departments that provide merchant services shall participate in the completion of the PCI requirements as well as the necessary follow-up for issues noted in the questionnaire and scan. Refer to the Annual Questionnaire and Quarterly Scan part in the Procedures section for additional information.*

A committee of ITS and Finance staff members have been working with campus departments on compliance with the data security standards. The initial focus has been on processes that use externally-facing IP addresses because internet applications require a quarterly scan of the application to test for security weaknesses that could allow breaches or place credit card data at risk. Below is the status of PCI compliance for campus credit card merchants using:

**Common Payment Service (CPS):** All active merchants with internet sites utilizing CPS are PCI compliant as of the date of this memo.

**Other Internet Gateways or Point of Sale Software:** All active merchants in this category are either PCI compliant or in the final stages of the certification process.

**Point of Sale (POS) Swipe Terminals:** These credit card merchants have NOT been certified as PCI compliant. Under a new directive from the Office of the State Controller, all credit card merchants in this category must now complete the *Payment Card Industry Self-Assessment Questionnaire* and be certified PCI compliant by the University. A separate memorandum with forms and instructions to attain compliance will be sent directly to these merchants (i.e. campus departments).

In order to transition to the new merchant card processing contract and to be compliant with both the Office of the State Controller and University policies, all campus credit card merchants shall:

1. Complete and submit a new Merchant Outlet Setup Form.
2. Be certified as compliant with the PCI Data Security Standards.

Departments that are directly impacted by these requirements will be contacted individually. **Any merchant determined to be non-compliant with the above will have the services associated with their merchant number terminated by SunTrust Merchant Services on October 31, 2006.**

This memorandum is being distributed to University business managers to ensure all departments are aware of the need for compliance with the credit card merchant services policies. Departmental staff members who perform credit card administrative duties may participate in a campus Listserve. To initiate or cease participation in the Credit Card Administrator Listserve, an email should be sent to [ccadm@unc.edu](mailto:ccadm@unc.edu). This restricted Listserve is only available to employees of the University of North Carolina at Chapel Hill who have managerial, administrative, or operational duties as a credit card merchant.

Thank you for your cooperation and assistance in this important matter.